Internal Controls 101

May 2014 Volume 1, Issue 1

Office of
Auditing Services

Inside this issue:

Special points of interest:

- Geared to the achievement of objectives
- Everyone has some level of responsibility
- The cost should not exceed the benefit

Internal Controls Defined

The Committee of Sponsoring Organizations of the Treadway Commission's (COSO) Definition:

Internal control is a process, effected by an entity's board of directors, management, and other personnel, designed to provide reasonable assurance regarding the achievement of objectives relating to operations, reporting, and compliance.

What?

Internal controls are simply those systems, processes, procedures, and mechanisms controlled by management that make it possible for the agency to successfully achieve its goals and objectives. These goals and objectives can be related to accurate **reporting** (financial or non-financial reporting), **compliance** with applicable laws and regulations, **efficiency and effectiveness** of operations and programs. Internal controls should be value-added and cost-effective.

While internal controls provide reasonable assurance of achieving the agency's objectives, limitations do exist. Internal controls cannot prevent poor judgment or decisions, or external events that could cause the agency to fail to achieve its operational objectives. Additionally, internal controls are limited by the ability of management to override them and collusion by internal personnel and/or third parties.

Responsibility

Who's responsible?

Everyone in the agency has some level of responsibility for internal controls. Management is responsible for making sure sound internal control structures are established, documented via written procedures, and implemented. An effective system of internal control demands more than rigorous adherence to policies and procedures- it requires the use of judgment. Management uses judgment to determine how much control is enough.

Staff is responsible for adhering to the established procedures and for reporting to management when controls are not working as designed.

Audit is responsible for assessing whether internal controls are present and functioning as designed and reporting those results to Management.

Why Do We Need Them?

Success does not just happen. Grant program and other operational managers do not achieve stated objectives and performance goals without processes and systems in place to mitigate the unexpected (risks). Management must develop objectives, identify the risks that may impact its ability to accomplish those objectives, and then design and implement controls to mitigate the risks that would have the greatest impact.

Both internal and external auditors will evaluate the adequacy of internal controls when your program or operation is audited. Typically, they will use the COSO framework to make this assessment.

The COSO framework is composed of five integrated components that support an organization in its efforts to achieve objectives: Control environment, Risk Assessment, Control Activities, Information and Communication, and Monitoring Activities. These components are relevant to the entire agency and to any individual operating unit, program, and function.

Internal Control is a process consisting of ongoing tasks and activities-a means to an end, not an end in itself.

The Components

The Control Environment is the set of standards, processes, and structures that provide the basis for carrying out internal control across the organization. It sets the tone of an organization.

Risk Assessment is management's formal process for assessing its operating environment and taking actions.

Control Activities are the actions established through policies and procedures that help ensure management's directives to mitigate risks to the achievement of objectives are carried out.

Information and Communication is the identification, capture, and exchange of information in a form and time frame that enables staff to carry out their internal control responsibilities.

Monitoring Activities are those ongoing or separate evaluations used to ascertain whether each component of internal control is present and functioning.

COSO 2013 defines 17 principles representing the fundamental concepts associated with each component.

So, what you're saying is…

Management is responsible for establishing, implementing, and maintaining an internal control structure that includes the components listed above. An effective system of internal control reduces, to an acceptable level, the risk of not achieving agency objectives. So, management is responsible for establishing a strong system of internal controls by:

- Exhibiting integrity and ethics (Control Environment);
- Appropriately assigning authority and responsibility (Control Environment);
- Committing to hire, train, and retain competent people (Control Environment);
- Establishing proper procedures to hold employees accountable for their actions (Control Environment);
- Specifying objectives with sufficient clarity to enable the identification of risks (Risk Assessment);
- Identifying risks that could impact those objectives, including fraud risks, and determining how to best manage those risks (Risk Assessment);

See *What You're Saying*, p. 3

What You're Saying (continued from p. 2)

- Selecting and developing controls to mitigate the risks (Control Activities);
- Selecting and developing controls over technology (Control Activities);
- Establishing controls through policies and procedures (Control Activities);
- Generating and using relevant quality information to make decisions (Information and Communication);
- Communicating appropriately internally and externally (Information and Communication);
- Performing ongoing monitoring to ensure components of internal control are working as designed (Monitoring Activities); and
- Evaluating and communicating internal control weaknesses to ensure needed changes are made (Monitoring Activities).

Examples of Objectives, Risks, and Controls

Assets

Objective: To ensure assets are properly safeguarded and recorded
Potential Risk: Employee theft or inventory obsolescence
Potential Controls: Assets, including inventory, cash, computers, low-value assets, and capital assets should be physically secured through the use of locks, safes, etc. A physical inventory should be conducted on a periodic basis. Assets and inventory records should be periodically reviewed for accuracy and obsolescence.

Reporting

Objective: To ensure accurate and complete financial reporting
Potential Risk: Incorrect data may be erroneously reported. Recognizing revenue and expenses in the wrong period could distort closing packages and other financial reporting. Inaccurate reporting may possibly impact future funding.
Potential Controls: Departmental reports should be reviewed for accuracy and errors should be resolved within established time frames. Accounts should be properly reconciled to supporting detail and differences should be appropriately researched and resolved.

It is not practical to design and implement a system of internal control unless objectives are established for the organization.

Grants Management

Objective: To successfully meet all funding requirements established by the funder in the approved budget
Potential Risk: Grant program budgets may be under or over expended, which may impact current and future funding, and subject the agency to reputational risk.
Potential Controls: Changes in regulatory requirements should be monitored to determine their applicability. Time and Effort reporting should be periodically validated. Grant program expenses should be regularly reviewed for compliance with the approved budget.

Data Access/Authentication

Objective: To protect employee and student data
Potential Risk: Data may be compromised, leading to disclosure of confidential employee or student information to unauthorized individuals. Sensitive information might be used for fraudulent purposes.
Potential Controls: Only authorized personnel should have access to sensitive and confidential data. System access levels should be assigned in accordance with job function and should be periodically reviewed by management. Strong passwords should be used to control access and user names and passwords should never be shared among employees.

See *Examples*, p. 4

Examples (Continued from p. 3)

Business Continuity/ Disaster Recovery

Objective: To ensure continued business operations with minimal interruptions
Potential Risk: Inability to recover lost critical data and resume core business functions. Inaccurate financial reporting due to loss of data.
Potential Controls: Disaster recovery and business resumption plans should be developed, tested, and maintained. Critical data and software should be backed up daily and rotated off-site.

Personnel Management

Objective: To ensure competent, professional, and well-trained resources exist
Potential Risk: Critical operations could be seriously interrupted by extended illness or separation of employment by key personnel.
Potential Controls: Key personnel should be appropriately cross trained. Roles and responsibilities should be defined, documented, and communicated to applicable personnel. Succession planning should exist.

Benefits

Effective internal control provides many benefits to an entity. It provides management with added confidence regarding the achievement of objectives. Other benefits include:

- Reliable reporting that supports management decision making
- Consistent mechanisms for processing transactions
- Increased efficiency within functions and processes
- A basis for decisions where highly subjective and substantial judgment is needed

Please visit http://www.coso.org/ for more information on COSO 2013.

Please feel free to contact us at auditingservices@ed.sc.gov with any questions or requests for additional information.